Amendments to the Specification:

Please replace paragraphs [0004], [0005], [0008], [0017], [0024] with the following amended paragraphs:

[0004] In many processing devices, such as computers, PDAs (personal digital assistants), mobile phones, and smart phones, it is necessary to maintain complete secrecy of certain data. One application, for example, would be financial transactions, where important information may be stored on the processing device or a memory external to the processing device. It is important that a third party could not access the processing device's memory in order to ascertain sensitive information. In some cases, there may be a need for information to be stored on the processing device that is to be maintained in secrecy even from the owner.

[0005] A typical method of storing sensitive information is by encryption. There are various encryption techniques, but a typical technique uses a "cipher" to encrypt data according to a "key". The cipher is the mathematical formula used to encrypt the data. The key is used by a cipher in the encryption.

[0008] Another technique is storing a ~~writing~~ previously generated random number to a memory on each integrated circuit at the time of manufacture. While this is an improvement, it would still be possible for those involved in the manufacturing stages of the processing circuit to trace keys to particular devices.

[0017] The random ~~memory~~ number generator 12 can be any conventional circuit that generates a random number responsive to the control signals. In the preferred embodiment, the event detector 14 observes the random number to detect situations where a possible tampering event has occurred or the random number generator 12 is defective, such as a number that has a ratio of "1"s to "0"s that is outside of a threshold. For example, if the ratio of "1"s to "0"s is below 113 or

above 213, the event detector may issue a NOK (not okay) signal, and the random number would be regenerated. Since the length of the random number is known, whether the ratio is above or below the thresholds can be determined by counting either the "1"s or "0"s in the generated random number and comparing the count to a threshold.

[0024] In operation, data is received through the RF and power circuitry 50, which generates digital data from the received analog signals. Certain data may be encrypted and decrypted using one or more programs stored in the memory subsystem 46 and executed on one of the processing circuits 44. Any access to the root key is made internally to the processing integrated circuit 42, such that the root key memory is not accessible through the I/O system 48, either directly or indirectly through the execution of malicious code on a programmable processing circuit 44. In one embodiment, the root key is not used directly to encrypt data (encrypt before storage), but is used to seed ~~(encrypt before storage)~~ another random number which becomes a session key. In this way, access to the root key by tampering with the code for one or more of the processors 44 is prevented.

Please replace the title with the following amended title:

~~On-Device Random Number Generator~~
Random Number and/or Key Generator on An Integrated Circuit